

GDPR/Data protection policy

1. Introduction

- 1.1 The law
- 1.2 Individuals rights
- 1.3 Managing data protection

2. Description of processing

- 2.1 Lawful basis for processing personal data / Consent
- 2.2 How we gather information

3. Reasons/purposes for processing information

- 3.1 Providing support and information for people affected by ovarian cancer
- 3.2 How we use your information

4. Type/ classes of information processed

- 4.1 We process information relevant to the above reasons/purposes.
- 4.2 We also process sensitive classes of information
- 4.3 What we process personal information about
- 4.4 Children's data

5. Who the information may be shared with

- 5.1 Other organisations and third parties
- 5.2 Sharing your story

6. Who had access to personal data

- 6.1 Processing personal data
- 6.2 Subject to access

7. Not kept longer than necessary

- 7.1 Data retention
- 7.2 Case study retention period when a person dies

8. Our commitment to data security: how we keep data safe

9. Data breaches

- 9.1 What is a data breach
- 9.2 Notifying a data breach
- 9.3 Informing an individual of a breach of their data

10. Transfers

1. Introduction

At Ovacome we are committed to keeping your personal data safe and protecting your privacy. This notice is made in light of the requirements of the Data Protection Act 1998 and the EU General Data Protection Regulation (GDPR) The purpose of these laws is to protect the rights of individuals, where their data (personal information) is obtained, stored and processed.

This policy provides guidance to ensure Ovacome staff process personal data in a safe and secure way which complies with current legislation and best practices. This policy applies to those who handle personal data, which includes Ovacome staff, trustees and volunteers.

1.1 The law

Data protection is essentially that area of the law that governs what may, and what may not, be done with personal information. Such personal information may be electronic form (stored on a computer) or manual form (stored in a manual filing system).

Ovacome fulfils the legal requirements by registering our details with the Information Commissioner's Office (ICO), adhering to the eight data protection principles and by educating all staff and volunteers in the correct use of personal data.

The Data Protection Act lists the data protection principles in the following terms:

- Principle 1: Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
 - (a) at least one of the conditions in Schedule 2 is met, and
 - (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
- Principle 2: Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Principle 3: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Principle 4: Personal data shall be accurate and, where necessary, kept up to date.

- Principle 5: Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Principle 6: Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Principle 7: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Principle 8: Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

1.2 Individual's rights

All individuals that Ovacome holds data on, has the right to:

- Be informed upon request of all the information held about them
- Prevent the processing of their data for the purpose of direct marketing
- The removal and correction of any inaccurate data about them

1.3 Managing data protection

Ovacome has an appointed Data Protection Officer (DPO) and Ovacome supports the data protection lead through provision of appropriate training and reporting mechanisms to senior management.

2. Description of processing

2.1 Lawful basis for processing personal data / Consent

Ovacome's lawful basis for processing personal data is consent. When you provide us with your personal information we will gain consent by asking you to select how we use your information and how we contact you.

We adhere to the legal requirements around gaining consent by being specific, granular, clear, and prominent, opt-in, properly documented and easily withdrawn.

2.2 How we gather information

With consent, when you provide us with your personal information we will gain consent by asking you to select how we use your information and how we contact you.

Directly, we collect personal information when you contact us directly or when you use our website to complete our web forms and we collect anonymous information including data on pages viewed, date and time and browser type for every visitor to our website.

Indirectly, your personal information may be shared with us by independent service providers, event organisers and fundraising sites like Just Giving, Virgin Money Giving, BT MyDonate, Squarespace and Health Unlocked. You can visit these organisations directly to view their full privacy policies but they will not share your information with us without your consent.

We also collect information when it is available from other public sources. We may collect personal data about you from the public domain, such as Companies house or the media.

These are some of the ways we collect personal data:

- Through responses to fundraising campaigns
- When you complete a membership registration form
- When you complete a donation forms
- Donating on a fundraising page
- Ordering patient information and materials
- Buying products from our shop
- Contributing to our newsletter
- Sending us an email
- Writing to us
- Phoning us
- Posting on our forum
- Completing our surveys
- Signing up to our events
- Signing up to receive our newsletters
- Signing up to volunteer with us

3. Reasons/purposes for processing information

3.1 Providing support and information for people affected by ovarian cancer

We process personal information to enable us to provide a voluntary service for the benefit of the national public as specified in our constitution; administer membership records; to fundraise and promote the interests of the charity; manage our employees and volunteers; maintain our own accounts and records.

3.2 How we use your information

Where you have given consent we will use your personal information in a number of ways including:

- To invite you to upcoming events
- To provide information about our services, products, campaigns and work
- To process requests for patient information and materials that we receive from you
- To invite you to participate in surveys and on advisory panels
- To process donations we may receive from you
- To invite you to participate in interactive features on our website
- For administrative purposes, including contacting you for an event you have registered to attend.
- For internal record keeping relating to donations, fundraising, complaints and feedback.

4. Type/classes of information processed

4.1 We process information relevant to the above reasons/purposes. This may include:

- personal details
- family details
- lifestyle and social circumstances
- membership details
- goods and services
- financial details
- education and employment details
- visual images, personal appearance and behaviour

4.2 We also process sensitive classes of information that may include:

- physical or mental health details
- racial or ethnic origin
- religious or other beliefs of a similar nature
- offences and alleged offences
- criminal proceedings, outcomes and sentences
- trade union membership

4.3 What we process personal information about

We process personal information about:

- members
- staff, volunteers
- supporters
- complainants, enquirers
- advisers
- representatives of other organisations

4.4 Children's data

Where appropriate we will seek consent from a parent or guardian before collecting information about children (anyone aged 18 or under). Information is usually collected when children attend our events or fundraise for us. We will collect name, date of birth and address in the same way we do for adults, to allow us to record the amount of support we have received.

5. Who the information may be shared with

5.1 Other organisations and third parties

We sometimes need to share the personal information we process with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA). What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

- If we run an event in partnership with another named organisation your details may need to be shared.
- We sometimes used external companies for mail services, like the posting of our newsletter.

We ensure we adhere to the legal requirements and best practice by using secure data transfer services and gaining informed consent when you register your information.

5.2 Sharing your story

Some people choose to tell us about their experiences to help contribute to our various campaigns and work. They may volunteer in our educational programmes, give talks at events, contribute to our newsletter, sit on an advisory panel and contribute to our publications. This involvement in our work means that people will often provide us with sensitive information.

Only with explicit consent of the individual, we will use some of the information provided to identify opportunities based on their expressed interest (including type of cancer, gender, age and contact information). This again with consent of the individual, or their parent or guardian if they are under 18, will be made public at our events and in our publications.

6. Who had access to personal data

6.1 Processing personal data

This policy operates on a “need to know” basis and apart from staff and volunteers in the Ovacome office; no-one will have access to client or organisational information unless it is relevant to the service or their work. Whenever Ovacome staff and volunteers process personal data, they will ensure that:

- If for any reason registration of the information is withdrawn they must stop using the particular data immediately.
- They must ensure that appropriate records are maintained and safe and are only used for their intended purpose.
- Information must be collected and processed in a prudent and lawful manner and should be kept up to date and accurate at all times
- The information should only be retained for the period necessary, and for the purpose for which it is held.

6.2 Subject to access

All individuals that Ovacome hold data on are entitled to make a ‘subject access’ request. Individuals have the right to ask for a copy of the information we hold about them (for which we may charge a small fee). Individuals can also ask for a description of their personal data, the reasons it is being processed, and whether it will be given to any other organisations or people.

Email requests are not accepted, individuals must provide a description of the information they want and proof of identity by post. Ovacome will respond to requests within all applicable timeframes (in accordance with the Information Commissioner’s Office guidelines).

In certain circumstances (e.g. where required or permitted by law) we might not be able to provide you with access to some of your personal information, but where appropriate we will notify you of the reasons for this.

7. Not kept longer than necessary

7.1 Data retention

We discourage the retention of data for longer than it is required. All personal data will be deleted or destroyed by us after it is no longer required for its intended purpose and/or no longer required to be kept by law.

7.2 Case Study retention period when a person dies

When a person (for whom we have a case study) dies, Ovacome will offer the consent form and any photos to the relatives of that person. We will never share a person's story after their death unless we have the consent of their relatives.

8. Our commitment to data security: how we keep data safe

All Ovacome computers have a log in system and our Database is password protected, which allows only authorised staff to access personal data. Passwords on all computers are changed frequently. All personal and financial data is kept in locked filing cabinets and can only be accessed by Ovacome staff.

We use secure systems to store information. And we keep it only for as long as is necessary for the purposes for which it was intended, or for as long as we are legally required to keep it.

Personally identifiable information is stored on our server and is not publicly accessible. Further, personally identifiable information is only accessed by Ovacome staff on a "need to know" basis. To prevent unauthorized access, maintain data accuracy, and ensure the correct use of information, we have put in place appropriate physical, electronic, and managerial procedures to safeguard and secure the information we collect online.

9. Data breaches

9.1 What is a data breach

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.

9.2 Notifying a data breach

A notifiable breach has to be reported to the relevant supervisory authority or if serious the Information Commissioner within 72 hours. If the breach is sufficiently serious to warrant notification to the public, Ovacome must do so without due delay.

What information must a breach notification contain?

- The nature of the personal data breach including where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- The name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, if the measures taken to mitigate any possible adverse effects.

9.3 Informing an individual of a breach of their data

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, those concerned directly will be notified by a senior member of the charity staff. A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

10. Transfers

It may sometimes be necessary to transfer personal information overseas. When this is needed information may be transferred to countries or territories around the world. Any transfers made will be in full compliance with all aspects of the data protection act.

Staff handbook copy

2B. CONFIDENTIALITY, COMMUNICATIONS, DATA PROTECTION AND EMAIL

1. The role of Ovacome is primarily to provide an information and support service to people with ovarian cancer. There is a presumption in all its work of sharing of research and other general medical-related information. However, in its relationships with individuals, and in particular with users of its information services, Ovacome recognises that there is a need for absolute confidentiality, and all staff and members of the Trustee Board are bound by all details of this confidentiality policy, and a breach of it will be considered as a potentially serious disciplinary offence
2. Confidentiality *within* Ovacome is also maintained at the highest appropriate level; in particular:
 - All confidential records are kept locked away at all times.
 - Personal details remain personal.
 - In accordance with its responsibilities under the Data Protection Act, any information collected by Ovacome will be used only for the purposes for which it was collected.
 - Ovacome mailing lists will not be revealed to third parties.Any employee or member of the Trustee Board in any doubt about an issue of confidentiality should first consult the Chief Executive before acting.
3. Any complaint by an outside organisation, service user or Trustee Board member against a member of staff will be investigated immediately and fully by the Chief Executive (or, in the case of a complaint against the Chief Executive, by the Chair of Trustees).
 1. Staff should not normally receive personal external post addressed to them at their workplace; arrangements for exceptions to this should as far as possible be agreed in advance with the Chief Executive. The organisation cannot be held responsible for any private correspondence lost in the office or opened in error.
 2. Staff using the organisation's e-mail and other electronic communication facilities should generally confine this use to Ovacome business, and may only use e-mail and access to the internet for personal purposes with discretion, in their own time and never when to do so would impact on their official responsibilities. Ovacome reserves the right to monitor all staff use of



ovarian cancer

e-mail, the internet and other means of communication, and will consider it a potential serious offence if material is accessed or generated that might bring the name of the organisation into disrepute.